Security of Foreign Intelligence in Automated Systems and Networks

(Effective _____)

Pursuant to section 102 of the National Security Act of 1947, Executive Order 12356, and National Security Council (NSC) Directives, this Director of Central Intelligence Directive (DCID) establishes policy and prescribes authority and responsibilities for the protection of foreign intelligence and counterintelligence (2). derived through sensitive sources and methods and processed, stored, or communicated by automated systems or networks (3).

Applicability

This Directive applies to all United States government departments and agencies which use automated systems to process, store, or communicate intelligence information. It applies with equal force to automated systems or networks owned or operated by the United States Government and those owned or operated by contractors or consultants performing for the United States Government.

POLICY

The rapid proliferation of automated tools and methods for the electronic processing of information demands that action be focused on providing security and surety for the intelligence information they contain and process equal to that heretofore applied to the manual and printed world. Automated systems and networks of the Intelligence Community (IC) will be managed and protected in a manner which insures that both the intelligence information and the sensitive sources and methods through which it is derived are effectively secured against successful attack by hostile intelligence activities. The goal of this Directive and the accompanying Regulation is to provide policy and broad technical guidance which will enforce the same classification, compartmentation, and need-to-know standards now applied to the manual handling of intelligence information.

the determination as to whether a specific system provides the required

1. Supercedes DCID 1/16, 6 June 1978
2. Foreign intelligence and counterintelligence are used in this directive as defined in Executive Order 12333 and as classified under the provisions of Executive Order 12356. For the purposes of this Directive, the term "intelligence information" shall include both foreign intelligence and foreign counterintelligence.
3. Automated systems and networks are defined as collections of computer-based equipment and sotware which are designed to process, store, or communicate information as digital data. Automated systems and networks include automated data processing (ADP), word processing (WP), automated office (AO), and electronic mail (EM) systems.

protection will be made by an individual NFIB member in single user systems/ networks and in collaboration with two or more NFIB members in cases of more complex interfaces.

The security modes outlined in the Regulation and the security standards and criteria mapped against those modes are neither prescriptive nor all-encompassing. They are guidelines pointing the systems/network designer toward tools, methods, and procedures which may be judiciously combined to achieve cost-effective protection for automated systems; they are pre-engineered solutions. Accreditation authorities will be allowed/required to accept some calculated risk, but may find its acceptance unpalatable unless it is defined with care and precision.

AUTHORITY

The NFIB members are assigned the following authority concerning automated systems/network accreditations:

Automated System/Network - The NFIB member who is the single user of an automated system/network is designated the Accreditation Authority for that system/network.

Multiple NFIB Members' System/Network - One NFIB member, selected by those NFIB members involved, will be designated as the Principal Accreditation Authority for that system/network.

NFIB Memebers' Concatenated Systems/Networks - When two or more systems/ networks are interconnected or when a system is connected to a network of systems, the NFIB members who are already designated as the Accreditation or Principal Accreditiation Authority of any of the systems/networks involved will become members of the Joint Accreditation Authority for the concatenated systems/networks. One of the NFIB members of the Joint Accreditation Authority will be designated, by joint agreement, Principal Joint Accreditation Authority and all participating NFIB members shall act as a common body for executing the responsibilities of the Joint Accreditation Authority.

RESPONSIBILITIES - The NFIB member(s) serving as Accreditation Authorities are responsible to:

a. Assure the most economical and effective utilization of NFIB resources while complying with the stated DCI policy.

b. Identify the information security requirements for the specific system/ network based on applicable intelligence information security policies and regulations.

c. Define the complete set of security measures/mechanisms required based on the functionality of the system/network, the user/operational environment, the information characteristics, and applicable information security criteria.

d. Perform the technical assessments, risk analyses, and security tests upon which an accreditation of the system/network can be granted.

e. Evaluate the system/network for compliance with this Directive and the standards/criteria established in the accompanying Regulation, and certify such compliance.

f. Accredit the system/network and establish the allowable operational environment based on the assessment and the security tests of the system/network.

g. Coordinate all system security actions to ensure that all managers and users of an automated system or network implement the established security measures and capabilities.

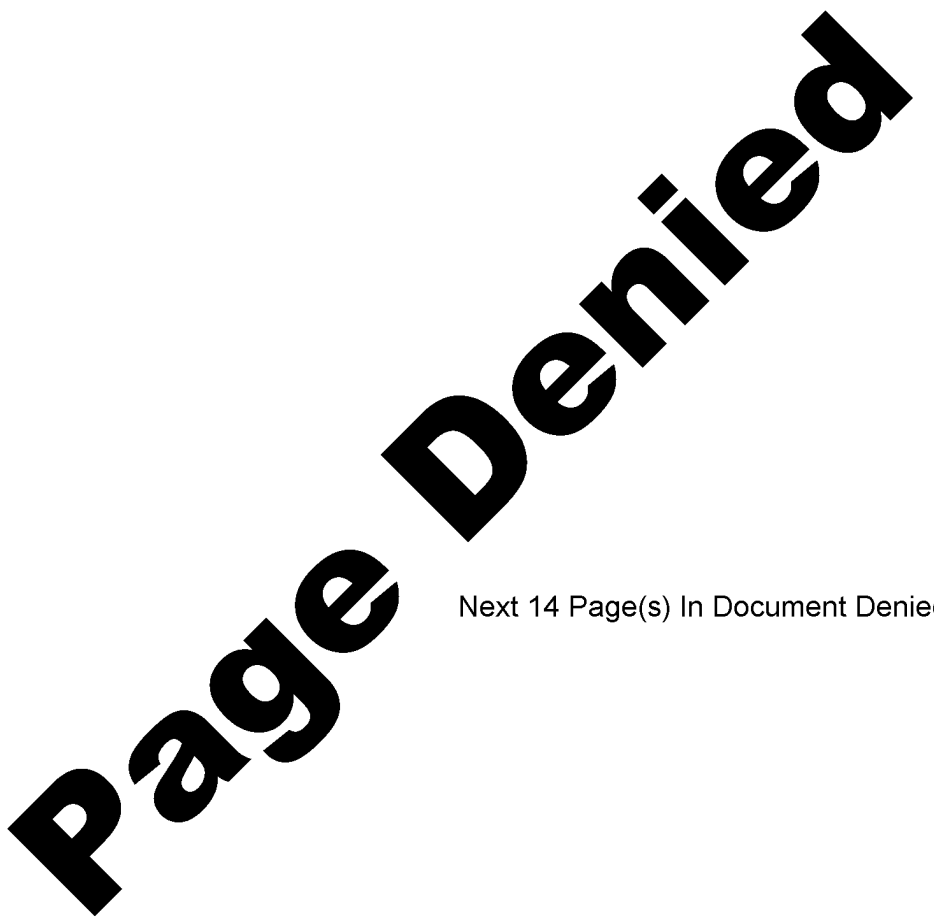
EXEMPTIONS - The NFIB member or his designee may temporarily exempt specific systems under his jurisdiction from complete compliance with this Directive and the accompanying Regulation when such compliance would significantly impair the execution of his mission. An exemption shall be granted only when the NFIB member or his designee has assured himself that the security measures in effect will adequately protect the intelligence information being processed in the specific automated system or network.

SUPERSESSION - This Directive supersedes Director of Central Intelligence Directive No. 1/16, "Security of Foreign Intelligence in Automated Data Processing Systems and Networks", effective 6 June 1978; and all existing directives, regulations, and other documents referencing the superseded Directive.

IMPLEMENTATION - Within one year of the effective date of this Directive each NFIB member will develop and promulgate a formal automated systems security program, implementing directives and regulations for systems and networks under his jurisdiction.

ADMINISTRATIVE REPORTS - Each NFIB member or his designee will provide to the Chairman, DCI Security Committee, an annual report as of 31 December detailing the accredited and exempted systems currently operating under his jurisdiction.

REVIEW - This Directive and the accompanying Regulation will be reviewed within three years from the effective date.



Next 14 Page(s) In Document Denied